

NIST Efficiency Testing of Round 2 AES Candidate Algorithms

Lawrence E Bassham III

Computer Scientist

Computer Security Division

NIST

April 13, 2000

ANSI C Testing: Cycle Count Measurements

- Generate 1000 of the following:
 - Cycles needed to generate a key for encryption
 - Cycles needed to encrypt n blocks of data
 - Cycles needed to generate a key for decryption
 - Cycles needed to decrypt n blocks of data
- Determine the median value for each of the four categories
- Average the values within 3 standard deviations of the median
- $n = 1, 16, 128, 1024, 32768$

ANSI C Testing: Timing Measurements

- Generate 1000 of the following:
 - Time needed to generate 100000 keys for encryption
 - Time needed to encrypt 1048576 blocks of data
 - Time needed to generate 100000 keys for decryption
 - Time needed to decrypt 1048576 blocks of data
- Determine the median value for each of the four categories
- Average the values within 3 standard deviations of the median

April 13, 2000

3

Platforms - LittleEndian

Processor/Hardware	Operating System	Compiler
200MHz Pentium® Pro Processor, 64MB RAM	Windows® 95	Borland C++ 5.01 Visual C++® 6.0
	Linux	GCC 2.8.1 (timing)
450MHz Pentium II Processor, 128 MB RAM	Windows98 4.10.1998	Borland C++ 5.01 Visual C 6.0
	Windows98 4.10.1998	Borland C++ 5.01 Visual C 6.0
800MHz Athlon™ Processor, 256MB RAM	Windows98 4.10.2222A	Borland C++ 5.01 Visual C 6.0

April 13, 2000

4

Platforms - BigEndian

Processor/Hardware	Operating System	Compiler
450MHz PowerPC G4 Processor w/ 1MB Cache, 384MB RAM	MacOS 9.0.2	CodeWarrior Pro Release 5
Sun™: 300MHz UltraSPARC-II™ w/ 2MB Cache, 128 MB RAM	Solaris™ 2.7	GCC 2.8.1
		Sun Workshop Compiler C™ 4.2
Sun: 2*360MHz UltraSPARC-II w/ 4MB Cache, 256 MB RAM	Solaris™ 2.7	GCC 2.8.1
		Sun Workshop Compiler C™ 4.2
Silicon Graphics™: 2*300MHz R12000™ w/ 4MB Cache, 512 MB RAM	IRIX64™ 6.5.4	GCC 2.8.1
		MIPSpro C Compiler 7.30

April 13, 2000

5

Compiler Options

- Compiler options as described in document
- Options for CodeWarrior Compiler:
 - ANSI Strict
 - Alignment: PowerPC
 - Target Processor: Generic PowerPC
 - Global Optimization: Faster Execute Speed
 - Level 4

April 13, 2000

6

Apple G4 PowerPC

Ekey, Dkey: Keys/msec; Encrypt, Decrypt: Mbit/sec

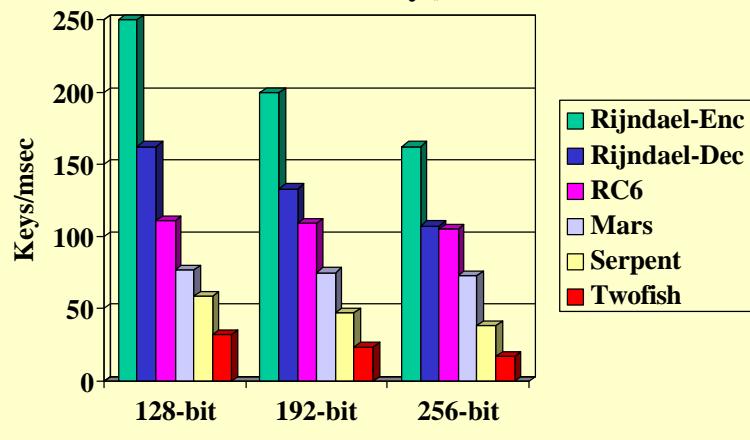
	Ekey	Encrypt	Dkey	Decrypt
Mars-128	76.9	80.6	76.9	83.9
Mars-192	75.0	80.6	75.0	83.9
Mars-256	73.2	80.6	73.2	83.9
RC6-128	111.1	125.9	111.1	123.9
RC6-192	109.2	125.9	109.2	123.9
RC6-256	105.3	125.9	105.3	123.9
Rijndael-128	250.0	52.6	162.3	57.1
Rijndael-192	200.0	44.3	133.3	47.9
Rijndael-256	162.3	38.2	107.2	41.3
Serpent-128	58.8	50.3	58.8	52.0
Serpent-192	46.9	50.3	46.9	52.0
Serpent-256	38.7	50.3	38.7	52.0
Twofish-128	31.9	50.3	32.1	47.9
Twofish-192	23.3	50.3	23.4	47.9
Twofish-256	17.4	50.3	17.4	47.9

April 13, 2000

7

Apple G4 PowerPC

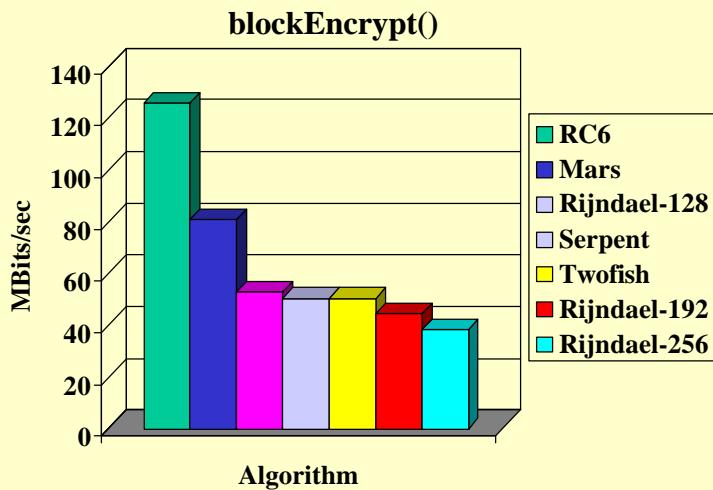
makeKey()



April 13, 2000

8

Apple G4 PowerPC



April 13, 2000

9

Athlon 800MHz Processor

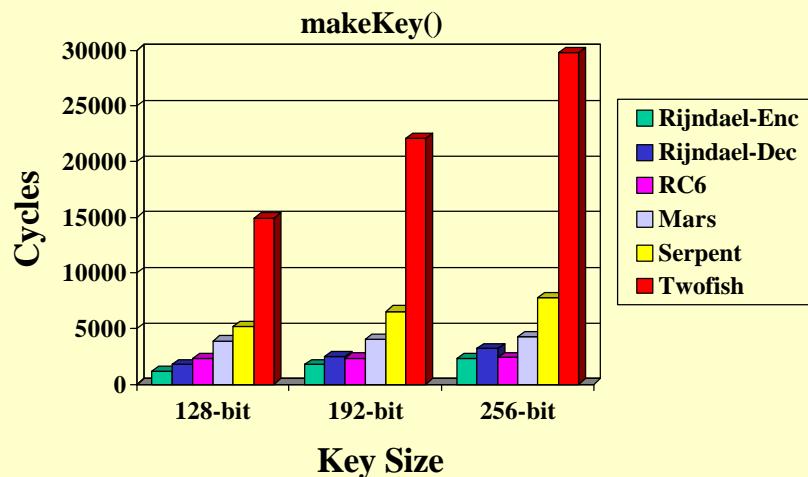
Visual C compiler, **cycle counts**, 128 blocks encrypted and decrypted (cycles per block)

	Ekey	Enc	Dkey	Dec
MARS-128	3860	585	3849	525
MARS-192	4008	585	3997	525
MARS-256	4237	585	4225	525
RC6-128	2248	318	2248	303
RC6-192	2317	318	2317	303
RC6-256	2390	318	2389	303
RIJNDAEL-128	1121	717	1720	740
RIJNDAEL-192	1732	883	2431	904
RIJNDAEL-256	2292	1035	3175	1058
SERPENT-128	5185	1073	5181	951
SERPENT-192	6540	1073	6582	951
SERPENT-256	7734	1073	7703	951
TWOFISH-128	14920	692	14895	627
TWOFISH-192	22042	692	21971	627
TWOFISH-256	29780	692	29693	626

April 13, 2000

10

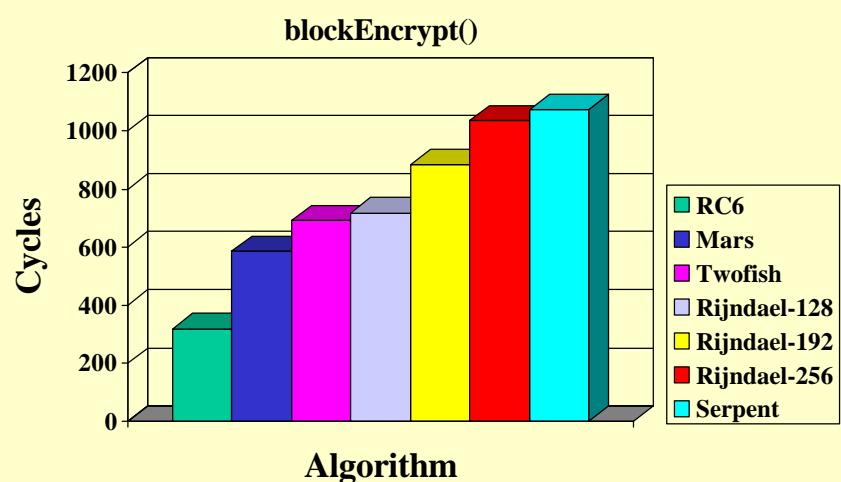
Athlon 800MHz - Visual C



April 13, 2000

11

Athlon 800MHz - Visual C



April 13, 2000

12

Platform Averages

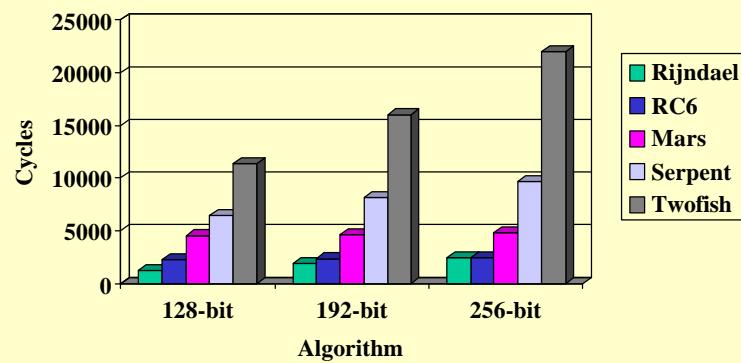
- Average key setup and encryption time over similar platforms
- Only encryption and key setup for encryption are provided
- Best times were selected
- Little-Endian Systems: Pentium Pro, Pentium III and Athlon
- Big-Endian Systems: PowerPC, RS12000 and UltraSPARC-II

April 13, 2000

13

Little-Endian Systems

Mean Cycle Count for makeKey() for Encryption

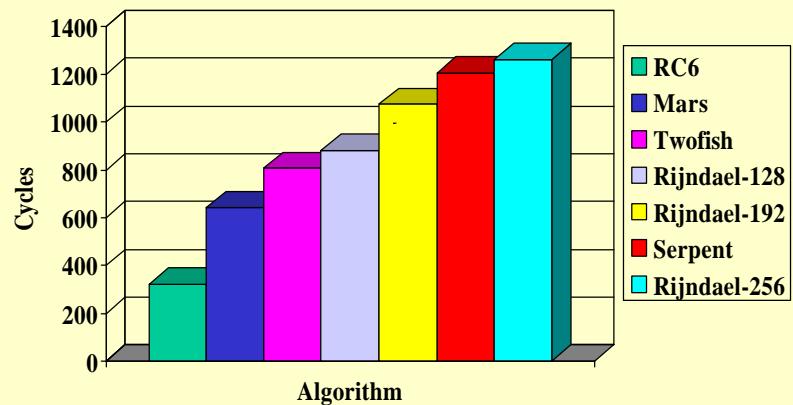


April 13, 2000

14

Little-Endian Systems

Mean Cycle Count for `blockEncrypt()`

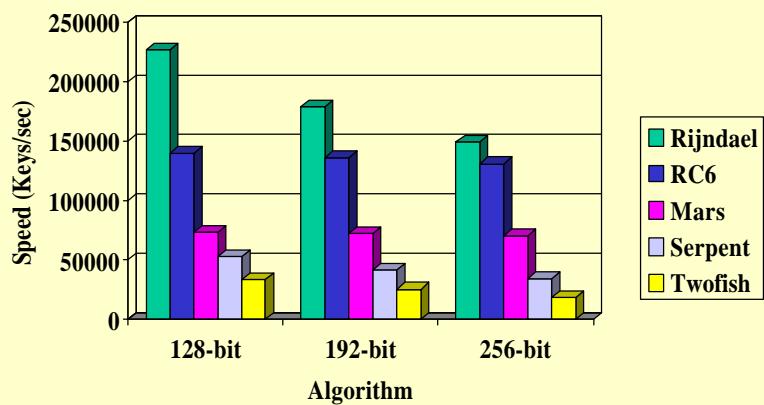


April 13, 2000

15

Big-Endian Systems

Mean Speed for `makeKey()` for Encryption

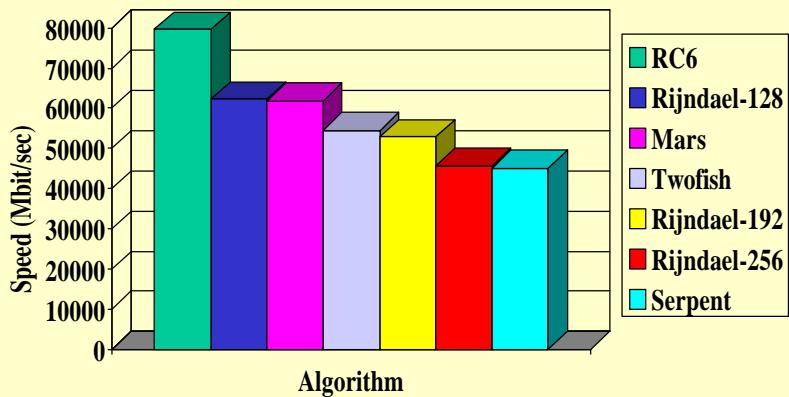


April 13, 2000

16

Big-Endian Systems

Mean Speed for blockEncrypt()



April 13, 2000

17

ANSI C Testing Conclusions

- RC6 performed constantly well in both key setup and encryption across platforms
- Rijndael is the clear winner on key setup across platforms
- Mars is an average to above average performer
- Twofish has poor key setup times and average encryption times across platforms
- Serpent has poor encryption times and below average key setup times across platforms
- These results must be weighed with results from other implementations and analysis

April 13, 2000

18

NIST's Java™ AES Analysis: Round Two

Reasons for using Java

- Java virtual machine isolates Java programs from differences between underlying hardware/OS platform
- Performance across different platforms is consistent
- For a given wordsize, linear relationship between performance and processor clock

NIST Final Round Test Setup

- Using Version 1.3 (JDK1.3 beta) of the Java Developer's Kit and Virtual Machine
- Reference platform specified by NIST
- NIST/Cryptix API
- Java source for candidates recompiled under JDK1.3 with no significant changes
- Analysis includes multiple key lengths (Round 1 limited to 128-bit keys)

April 13, 2000

21

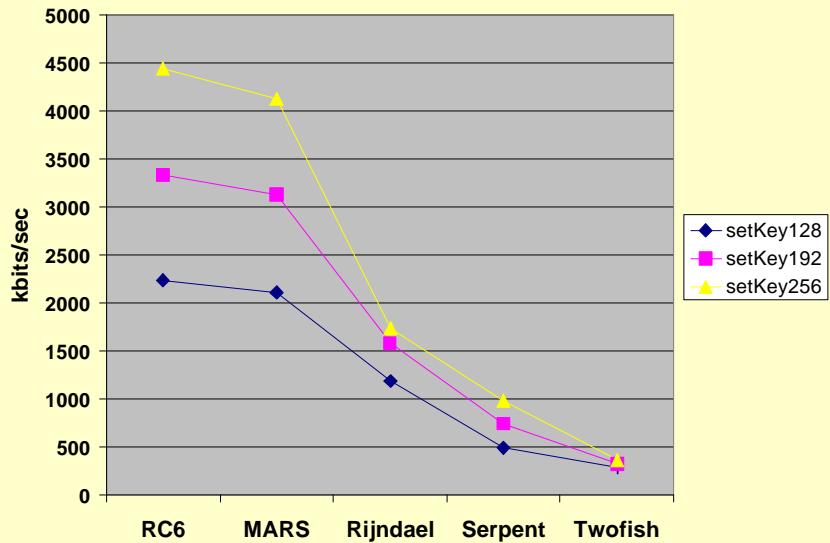
Test Procedures

- Compile candidates under JDK1.3 (beta)
- Execute 500,000 cycles of each candidate/keysizes/crypto-op combination
- Obtain start/stop times by calling System.time.millis()

April 13, 2000

22

Chart 1: Key Setup



April 13, 2000

23

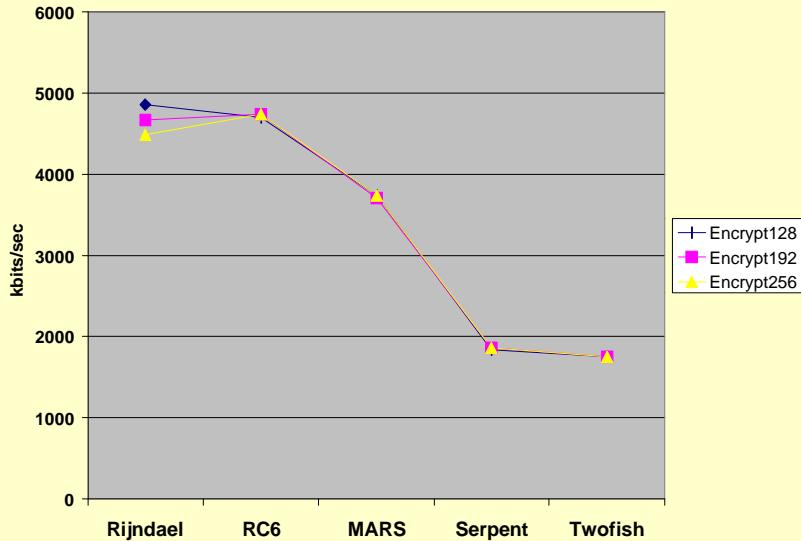
Results: 128-Bit Key Setup

- JDK1.1.6
 - Rijndael, RC6, MARS, Twofish, Serpent
- JDK1.3
 - RC6, MARS, Rijndael, Serpent, Twofish
- (Ordered from fastest to slowest)

April 13, 2000

24

Chart 2: Encrypt Operations



April 13, 2000

25

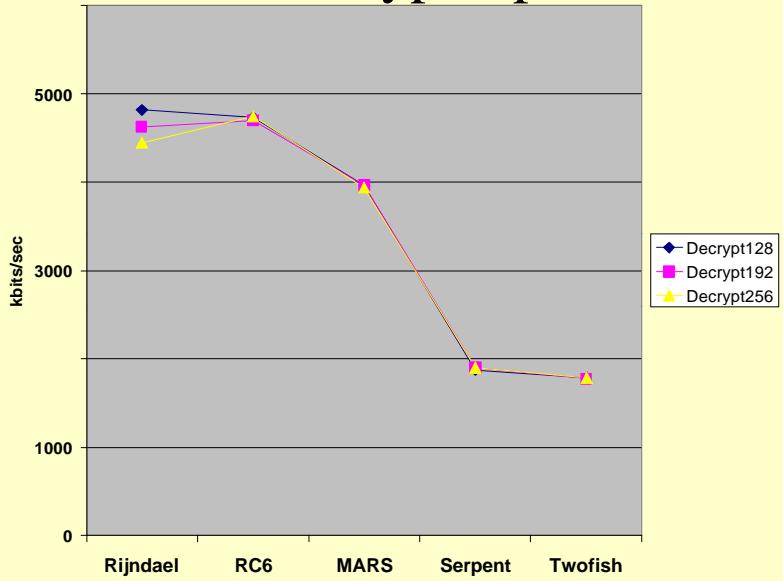
Results: 128-Bit Encrypt

- JDK1.1.6
 - RC6, Rijndael, MARS, Serpent, Twofish
- JDK1.3
 - Rijndael, RC6, MARS, Serpent, Twofish
- (Ordered from fastest to slowest)

April 13, 2000

26

Chart 3: Decrypt Operations



April 13, 2000

27

Results: 128-Bit Decrypt

- JDK1.1.6
 -
-
- JDK1.3
 - Rijndael, RC6, MARS, Twofish, Serpent

April 13, 2000

Notes for MARS

- New version tested under JDK1.1.6/JDK1.3
- Raw data for MARS/JDK1.1.6 re-test:

Key Size	Key Setup (ms)	Encrypt (kbytes/sec)	(kbytes/sec)
128 bits	165	462	444
192 bits	244	466	444
256 bits	324	465	445

29

Other Java AES Efforts

- and Lipp
- Complementary work using:
 - Hand-optimized implementations
 - JDK1.2 (Java 2)
 - Windows™ NT
 -

Conclusion

NIST and IAIK papers agree that Java™ AES implementations will be important. These results give a perspective on performance of the AES candidates in a language and execution environment that is dramatically different from traditional compiled/assembled languages such as C or assembler.

April 13, 2000

31

Contacts

- ANSI C testing questions:
 - Larry Bassham <lbassham@nist.gov>
- Java testing questions:
 - Jim Dray <jdray@nist.gov>

April 13, 2000

32